EXHIBIT #5

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Texas

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* FIVE CELLULAR TELEPHONES CURRENTLY IN THE CUSTODY OF THE FEDERAL BUREAU OF INVESTIGATION	)	Case No. A:16-m-733

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the WESTERN District of TEXAS *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

YOU ARE COMMANDED to execute this warrant on or before _____ *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Mark Lane.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 10-3-2016 1:30 p.m.

_____
Judge's signature

City and state: Austin, TX

Mark Lane, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

1. The devices to be searched are as follows: 1) SAMSUNG GALAXY NOTE 5 WITH SIM CARD 8901260415764302408; 2) APPLE IPHONE MODEL A1586 WITH IMEI 352061066787330; 3) APPLE IPHONE MODEL A1524 WITH IMEI 354376061250144; 4) ALCATEL ONE TOUCH 665A WITH IMEI 013088004400263 AND 5) SAMSUNG GALAXY NOTE 4 WITH SIM CARD 8901260312783924447. The Devices are currently stored at the FBI's Austin Resident Agency, located at 12515 Research Boulevard, Austin, Texas.

2. This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of Conspiracy to Conduct or Participate in an Enterprise Engaged in a Pattern of Racketeering Activity, in violation of Title 18, United States Code 1962(d), Conspiracy to Commit Wire Fraud, in violation of Title 18, United States Code 1349 and 1343, Aggravated Identity Theft, in violation of Title 18, United States Code 1028A(a)(1), and Attempted Capital Murder, in violation of Texas Penal Code and involve Chimene Onyeri, Marcellus Antoine Burgin and Rasul Kareem Scott and any known or unknown accomplices, co-conspirators, witnesses, victims and/or criminal associates, including evidence, fruits and instrumentalities of the offenses described herein, including but not limited to contact lists, call logs, voicemails, e-mails, files, communications, records, text messages, photos, audios, videos, images, notes, Internet browsing data, device data, operating system data, application data network data and locational data related to and in furtherance of the offenses described herein, in any form.

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

AO 106 (Rev. 04/10) Application for a Search Warrant

Sealed

FILED
16 OCT -3 PM 1:29
CLERK, U.S. DISTRICT COURT
WESTERN DISTRICT OF TEXAS
BY _____
DEPUTY CLERK

UNITED STATES DISTRICT COURT

for the

Western District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

FIVE CELLULAR TELEPHONES CURRENTLY IN THE CUSTODY OF THE FEDERAL BUREAU OF INVESTIGATION

Case No. A:16-m-733

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A

located in the Western District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18 USC, Section 1962(d)	RICO CONSPIRACY
Title 18 USC, Section 1349	WIRE FRAUD CONSPIRACY
TPCS Sections 15.01 etc...	ATTEMPTED CAPITAL MURDER

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Daniel D. Brust
Printed name and title

Sworn to before me and signed in my presence.

Date: 10-3-2016

Judge's signature

City and state: Austin, TX

Mark Lane, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

1. The devices to be searched are as follows: 1) SAMSUNG GALAXY NOTE 5 WITH SIM CARD 8901260415764302408; 2) APPLE IPHONE MODEL A1586 WITH IMEI 352061066787330; 3) APPLE IPHONE MODEL A1524 WITH IMEI 354376061250144; 4) ALCATEL ONE TOUCH 665A WITH IMEI 013088004400263 AND 5) SAMSUNG GALAXY NOTE 4 WITH SIM CARD 8901260312783924447. The Devices are currently stored at the FBI's Austin Resident Agency, located at 12515 Research Boulevard, Austin, Texas.

2. This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of Conspiracy to Conduct or Participate in an Enterprise Engaged in a Pattern of Racketeering Activity, in violation of Title 18, United States Code 1962(d), Conspiracy to Commit Wire Fraud, in violation of Title 18, United States Code 1349 and 1343, Aggravated Identity Theft, in violation of Title 18, United States Code 1028A(a)(1), and Attempted Capital Murder, in violation of Texas Penal Code and involve Chimene Onyeri, Marcellus Antoine Burgin and Rasul Kareem Scott and any known or unknown accomplices, co-conspirators, witnesses, victims and/or criminal associates, including evidence, fruits and instrumentalities of the offenses described herein, including but not limited to contact lists, call logs, voicemails, e-mails, files, communications, records, text messages, photos, audios, videos, images, notes, Internet browsing data, device data, operating system data, application data network data and locational data related to and in furtherance of the offenses described herein, in any form.

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

IN THE MATTER OF THE SEARCH OF: (1) SAMSUNG GALAXY NOTE 5 WITH SIM CARD 8901260415764302408; (2) APPLE IPHONE MODEL A1586 WITH IMEI 352061066787330; (3) APPLE IPHONE MODEL A1524 WITH IMEI 354376061250144; (4) ALCATEL ONE TOUCH 665A WITH IMEI 013088004400263; AND (5) SAMSUNG GALAXY NOTE 4 WITH SIM CARD 8901260312783924447, ALL CURRENTLY LOCATED AT THE FEDERAL BUREAU OF INVESTIGATION, AUSTIN, TEXAS.

Case No. A-16-m-733

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Daniel D. Brust, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—five (5) electronic devices—which are each currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation, and have been since August 11, 2002. I am currently assigned to the San Antonio Division, Austin Resident Agency, White Collar Crime Squad. I have investigated criminal activities with a nexus to fraud in the Western District of Texas and elsewhere. I have participated in all aspects of criminal

investigations, including, but not limited to analyzing information obtained from court ordered pen registers and trap and trace devices, analyzing telephone toll records, analyzing historical cellular tower information, and conducting court ordered wire intercepts of both voice and data communications. I have received training and have experience in the methods employed by individuals and groups engaged in criminal activities, to include their methods of communication and methods of avoiding detection by law enforcement.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The devices to be searched are as follows: 1) SAMSUNG GALAXY NOTE 5 WITH SIM CARD 8901260415764302408; 2) APPLE IPHONE MODEL A1586 WITH IMEI 352061066787330; 3) APPLE IPHONE MODEL A1524 WITH IMEI 354376061250144; 4) ALCATEL ONE TOUCH 665A WITH IMEI 013088004400263; AND 5) SAMSUNG GALAXY NOTE 4 WITH SIM CARD 8901260312783924447, hereinafter collectively referred to as ("The Devices"). The Devices are currently stored at the FBI's Austin Resident Agency, located at 12515 Research Boulevard, Austin, Texas, within the Western District of Texas.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. The FBI, Internal Revenue Service Criminal Investigations (IRS-CI), United States Postal Inspection Service (USPIS), Austin Police Department (APD) and other state, local

and federal agencies are investigating, Chimene Onyeri (Onyeri), Marcellus Antoine Burgin (Burgin) and Rasul Kareem Scott (Scott) for, among other things, Conspiracy to Conduct or Participate in an Enterprise Engaged in a Pattern of Racketeering Activity, in violation of Title 18, United States Code 1962(d) "RICO Conspiracy", Conspiracy to Commit Wire Fraud, in violation of Title 18, United States Code 1349 and 1343, Aggravated Identity Theft, in violation of Title 18, United States Code 1028A(a)(1), as well as Attempted Capital Murder, in violation of the Texas Penal Code, hereinafter "The Offenses." Pursuant to this investigation, on September 20, 2016, Onyeri, Burgin and Scott were indicted by a Federal Grand Jury sitting in the Western District of Texas for one count RICO Conspiracy, one count Conspiracy to Commit Wire Fraud and one count Aggravated Identity Theft. Your affiant believes that Onyeri is the leader of the criminal enterprise engaged in the aforementioned violations and other related federal and state offenses, including the attempted Capital Murder of a sitting Travis County District Court Judge on or about November 6, 2015. The criminal investigation of Onyeri, Burgin and Scott reveals, among other things, that all three participated in the attempted murder of the Travis County Judge and that Onyeri, Burgin and Scott all participated in a conspiracy to commit wire fraud as well as identity theft, as part of a debit card skimming fraud scheme.

7. In March, 2012, the Rollingwood Police Department (RPD), located in Travis County, Texas, within the Western District of Texas, conducted a traffic stop of a vehicle occupied by Onyeri and another individual. As a result, the RPD located and seized from the vehicle approximately seventy-seven gift cards, credit cards and/or counterfeit credit cards, many of which were encoded with or purchased with stolen credit and/or debit card numbers. It was later determined by law enforcement officers that the stolen card numbers were obtained *via* "skimming" from victims in the Houston, Texas area. The skimming was accomplished through

accomplices working at restaurants or retail establishments who used a device that allowed swiped credit card numbers of unsuspecting victims to be captured and stored. Subsequently, Onyeri was arrested and charged in the 390th District Court of Travis County, Texas for Fraudulent Use of Identifying Information (2nd Degree Felony). Onyeri received a sentence of three (3) years deferred adjudication from the Honorable Julie Kocurek. On August 28, 2015 a motion to proceed with an Adjudication of Guilt was filed in the 390th District Court and the case was set on the court's docket on October 7, 2015.

8. On the evening of November 6, 2015, Judge Kocurek was shot multiple times at her residence in Austin, Texas. Judge Kocurek was seriously wounded, but survived her injuries. Based on the investigation conducted by the FBI, IRS-CI, USPIS, APD and others, your affiant believes that Onyeri shot Judge Kocurek. Additionally, as set out herein, your affiant believes that Burgin and Scott were accomplices in the attempted murder of Judge Kocurek.

9. Immediately following the shooting of Judge Kocurek, the APD processed the crime scene and canvassed the area for witnesses. A witness observed a silver colored, four-door vehicle flee from the scene of the shooting with multiple occupants.

10. In the days after the attempted murder of Judge Kocurek, law enforcement received information from a confidential informant (CI#1). Your affiant deems CI#1's information to be credible and reliable[1]. CI#1 reported that Onyeri, a Houston area resident, was

[1] CI#1 participated in fraudulent financial activity with Onyeri in approximately the Spring, 2015. CI#1 has agreed to cooperate but has not pleaded guilty to any offense related to this investigation nor testified before the Grand Jury. CI#1 is currently under state supervision for charges related to felony Credit Card Abuse and Aggravated Assault with a Deadly Weapon. Much of the information provided by CI#1 has been corroborated by information provided by other witnesses, cellular phone records, and/or other collected evidence.

boasting about shooting Judge Kocurek. Subsequent investigation revealed that Onyeri utilized cellular telephone number (832) 335-2534 (Onyeri's phone) during this time period. Among other sources of information, Onyeri's own father told investigators that this was Onyeri's cellular phone number. Pursuant to a search warrant, the Austin Police Department, obtained from T-mobile the following: subscriber information, historical toll records, and historical tower information for Onyeri's phone during the time period prior to and subsequent to the shooting of Judge Kocurek. The SAMSUNG GALAXY NOTE 5 WITH SIM CARD 8901260415764302408 listed herein is associated with (832) 335-2534.

11. On or about November 9, 2015, Onyeri was arrested in Houston, Texas pursuant to an active felony warrant out of the state of Louisiana. At the time of his apprehension, Onyeri was in a vehicle, occupied by Burgin, Henry Yehe (Yehe) and another male. Subsequent to the traffic stop, law enforcement executed a warrant at Yehe's apartment. During the search numerous items related to credit card fraud and credit card skimming were seized.

12. On or about November 10, 2015, law enforcement executed a search warrant for the vehicle in which Onyeri was apprehended (silver 2012 Dodge Charger with Texas License Plate number DBP8855). During the search, four damaged cellular telephone devices were recovered. Onyeri told investigators that he and the other occupants of the vehicle attempted to destroy the phones when they realized law enforcement might stop the car in which they were traveling. These four mobile phones are four of the Devices listed in this affidavit (SAMSUNG GALAXY NOTE 5 WITH SIM CARD 8901260415764302408, APPLE IPHONE MODEL A1586 WITH IMEI 352061066787330, APPLE IPHONE MODEL A1524 WITH IMEI 354376061250144, ALCATEL ONE TOUCH 665A WITH IMEI 013088004400263). The fifth

phone (SAMSUNG GALAXY NOTE 4 WITH SIM CARD 8901260312783924447) was seized at Onyeri's residence located at 12383 Wellington Park, Houston, Harris County, Texas, pursuant to another authorized search warrant which was executed on or about November 11, 2015.

13. On or about November 13, 2015, Travis County District Attorney Investigator Sergeant Manuel Fuentes, a certified cellular forensic examiner, examined the Devices. Sergeant Fuentes was able to forensically determine that one of the recovered devices, an APPLE IPHONE MODEL A1586 WITH IMEI 352061066787330, was assigned telephone number [redacted] (Burgin's phone), and as set out above, the SAMSUNG GALAXY NOTE 5 WITH SIM CARD 8901260415764302408 was associated with telephone number (832) 335-2534. Pursuant to a search warrant, the APD obtained from Sprint Corporation the following: subscriber information, historical toll records and historical cellular tower information for Burgin's phone during the time period prior to and subsequent to the shooting of Judge Kocurek. According to Sprint Corporation, Burgin's phone was subscribed by Marcellus Burgin and billed to Burgin's known residence.

14. The APD conducted an analysis of historical call logs and historical tower information for Onyeri and Burgin's phones for the time period prior to and subsequent to the shooting of Judge Kocurek. Based on this analysis, APD Detective Derek Israel determined telephone number [redacted] (Scott's phone) to be pertinent to the investigation. Pursuant to a search warrant, the APD obtained from T-mobile the following: subscriber information, historical toll records, and historical cellular tower information for Scott's phone during the time period prior to and subsequent to the shooting of Judge Kocurek. According to T-mobile, Scott's

phone was subscribed by Rasul Scott and billed to the known residence of Scott. This phone was not recovered in the Houston area searches.

15. Among other things, the analysis of the cellular telephone tower records link Onyeri, Burgin, and Scott to both a debit card skimming scheme as well as the shooting of Judge Kocurek. Further, as set out below, cellular telephone tower records from October, 2015, through November 6, 2015, link Onyeri, Burgin and Scott to each other and to the events leading up to the shooting of Judge Kocurek.

16. Travis County District Court records revealed Onyeri appeared before Judge Kocurek in Austin, Texas on October 7, 2015. Onyeri's phone records also showed cellular tower connections in Austin, Texas on October 7, 2015. Following the court appearance, Onyeri's cellular telephone records indicated Onyeri returned to Houston, Texas. Numerous witnesses have informed investigators that after arriving back in Houston, Onyeri stated that he wanted to kill Judge Kocurek because she was going to send him back to jail. CI#1 reported this to authorities before the attempted murder of Judge Kocurek.

17. An additional confidential informant (CI#2) was developed by law enforcement. Your affiant deems CI#2's information to be credible and reliable[2]. CI#2 informed the FBI that in October, 2015, while CI#2 acted as a lookout, Onyeri attached a skimming device to an Automatic Teller Machine (ATM) located at an Amegy Bank in Houston, Texas. CI#2 described

[2] CI#2 participated in fraudulent financial activity with Onyeri from approximately the middle of 2014 to approximately October, 2015. CI#2 has agreed to cooperate but has not pleaded guilty to any offense related to this investigation nor testified before the Grand Jury. CI#2 has no felony convictions. Much of the information provided by CI#2 has been corroborated by information provided by other witnesses, cellular phone data and/or other collected evidence.

the vehicle that Onyeri used to drive up to the ATM and also described the approximate location of the bank. A review of Onyeri's phone records and bank surveillance recordings confirm that Onyeri was at or near the Amegy Bank in Houston, Texas on or about October 17, 2015, as described by CI#2. Other cellular phone records demonstrate and corroborate the fact the CI#2 was present with Onyeri on or about October 17, 2015, at the time of this skimming. Bank records demonstrate that approximately sixteen (16) debit card numbers were skimmed while the skimming device was attached to the ATM at Amegy Bank described by CI#2 on October 17, 2015. Two of these card numbers were subsequently exploited by Onyeri, Burgin and Scott.

18. On or about October 24, 2015, three money orders, totaling approximately $2,500, were purchased using banking information stolen from the Amegy Bank on or about October 17, 2015. The money orders were purchased at a Walmart in Houston, Texas, and subsequently negotiated at the L'Auberge Casino in Lake Charles, Louisiana on November 4, 2015. All three of these money orders were negotiated by Burgin, using his own Driver's License. Burgin's cellular telephone phone tower records also indicate that Burgin was at the L'Auberge Casino on November 4, 2015, through November 5, 2015.

19. On or about October 25, 2015, three money orders, totaling approximately $2,500, were purchased using banking information stolen on October 17, 2015. One of these money orders was negotiated by Burgin at the L'Auberge Casino using his own Driver's License and two were negotiated by Scott. Scott's signature appears in the signature block of the negotiated money order. The money order was negotiated at a check cashing store in Houston, Texas.

20. On or about October 26, 2015, three money orders, totaling approximately $2,500, were purchased using banking information stolen on October 17, 2015. All three were negotiated in the Houston area by Scott. Scott used his Louisiana Driver's License to negotiate one of these money orders and the other two had Scott's name signed in the signature blocks.

21. On or about October 30, 2015, Onyeri's cellular phone tower records indicate Onyeri was in Austin, Texas and was in the area of Judge Kocurek's home. There is no known legitimate reason for Onyeri to be in or near Judge Kocurek's residence or neighborhood. Additionally, Burgin's phone connected to a cell tower located near La Grange, Texas on October 30, 2015. Your affiant notes that a common route from Houston to Austin would go through La Grange, Texas. Additionally, Onyeri's phone records show that this was the route that he appeared to take from Austin to Houston on October 30, 2015. Based on this information, your affiant believes that Burgin traveled to Austin with Onyeri for the purpose of conducting surveillance of Judge Kocurek in preparation for her shooting and/or to murder Judge Kocurek.

22. On or about November 2, 2015, funds were withdrawn from an Amegy Bank account associated with the stolen banking information that was skimmed on or about October 17, 2015 and described above. The transactions were conducted at numerous locations in the Houston, Texas area. Based on analysis of Onyeri, Burgin, and Scott's phone cellular tower records, your affiant believes Onyeri, Burgin, and Scott traveled together on November 2, 2015, as they conducted the fraudulent financial activity. This fraudulent financial activity included ATM transactions, the purchase of money orders, and the purchase of gift cards.

23. On or about November 3, 2015, three money orders, totaling approximately $2,600, were purchased using banking information skimmed and stolen on October 17, 2015. Based on analysis of cellular telephone tower records, your affiant believes Onyeri, Burgin, and Scott congregated at a location in Houston, Texas on November 3, 2015, after these money orders were purchased. All three of these money orders were negotiated by Burgin, using his Driver's License, at the L'Auberge Casino in Lake Charles, Louisiana on November 4, 2015.

24. On November 3, 2015, a silver, four-door vehicle was rented from a Houston area Enterprise Rental location in the name of Onyeri's father – Innocent Onyeri. Onyeri and his father can both be seen on video surveillance recordings at the rental car location.

25. On or about November 4, 2015, Onyeri, Burgin, and Scott were at the L'Auberge casino located in Calcasieu Parish, Louisiana. This information is corroborated by cellular telephone tower records, casino surveillance video, and casino transaction records.

26. Based upon the analysis of cellular telephone records, your affiant believes that Onyeri, Burgin, and Scott together traveled from Louisiana to Houston, Texas then to Austin, Texas on or about November 5, 2015. The three were in the area of Judge Kocurek's residence on the afternoon and/or early evening of November 5, 2015. This information was determined thorough the analysis of Onyeri's, Burgin's, and Scott's phone cellular tower records.

27. On or about November 5, 2015, Onyeri was captured on surveillance video purchasing gloves at an Auto Zone in Austin, Texas. Onyeri used one of the two (2) gift cards purchased on November 2, 2015, to purchase the gloves. Also on November 5, 2015, Onyeri and Scott were captured on video together at a WalMart in Austin, Texas. Before leaving

WalMart together, Scott used one of the two (2) gift cards purchased on November 2, 2015, to purchase shoes, clothing and other items.

28. At approximately 6:43 pm, on November 5, 2015, Onyeri's phone number made two calls to Judge Kocurek's residence. Onyeri, Burgin, and Scott's phone cellular tower records indicate they were in the vicinity of Judge Kocurek's residence around the time these telephone calls were placed.

29. In the evening, on November 5, 2015, Onyeri, Burgin, and Scott checked into an Austin, Texas area Motel 6. Scott paid for the room using a gift card which was purchased using bank information stolen from the Amegy Bank on October 17, 2015. Scott provided his Driver's License as identification at check-in. Surveillance video from the Motel 6 captured Onyeri, Burgin, Scott, the clothes they were wearing, and the vehicle they were using. The vehicle's appearance is consistent with the vehicle rented from Enterprise Rental on November 3, 2015, as well as the vehicle described by some witnesses who reported suspicious activity in Judge Kocurek's neighborhood before and immediately after the shooting.

30. At approximately 11:41 am, on November 6, 2015, Onyeri, Burgin, and Scott were captured on surveillance video leaving the Motel 6.

31. Based on the analysis of Onyeri's, Burgin's, and Scott's phone cellular tower records and a review of witness statements, your affiant believes Onyeri, Burgin, and Scott together surveilled and stalked Judge Kocurek for hours before the attempted murder of Judge Kocurek on November 6, 2015. The first 911 call reporting the shooting of Judge Kocurek was received at 10:16 pm, on November 6, 2015.

32. Your affiant believes Onyeri, Burgin, and Scott returned to Onyeri's residence in Houston, Texas following the shooting of Judge Kocurek. This information is based upon an analysis of Onyeri, Burgin, and Scott's phone cellular tower records, among other things. Based on these same records, your affiant believes that Burgin and Scott went to Burgin's residence sometime after leaving Onyeri's residence.

33. An additional confidential informant (CI#3) was developed by law enforcement. Your affiant deems CI#3's information to be credible and reliable[3]. CI#3 was present at Onyeri's residence during the early morning hours on November 7, 2015. CI#3 informed investigators that also present at Onyeri's residence was a black/male Onyeri referred to as "N.O." and a black/male Onyeri referred to as "Southwest." Your affiant believes "N.O." is a nickname for Scott due to Scott being from New Orleans and "Southwest" is a nickname for Burgin due to Burgin being from Southwest Houston. CI#3 related a conversation in which Onyeri, "N.O.", and "Southwest" provided details regarding the shooting of Judge Kocurek that I know only the perpetrators and/or law enforcement would know. CI#3 learned these details directly from Onyeri, "N.O.", and "Southwest." CI#3 also stated Onyeri returned a rental car to Enterprise Rental on November 7, 2015. CI#3 was able to identify a photograph of Scott as the individual "N.O." but did not identify Burgin's photograph. CI#3 stated that he was fifty percent sure that Scott was the person Onyeri introduced as "N.O."

---

[3] CI#3 participated in fraudulent financial activity with Onyeri from approximately the middle of 2013 to August, 2014. CI#3 has agreed to cooperate but has not pleaded guilty to any offense related to this investigation. CI#3 was questioned in the Harris County, Texas Grand Jury about matters related to this investigation. CI#3 lied during those proceedings, and has admitted to such. CI#3 was recently released from custody in Calcasieu Parish, Louisiana, where CI#3 is facing racketeering charges under a state racketeering statute. In May, 2015, CI#3 received deferred adjudication for felonious Forgery. Much of the information provided by CI#3 has been corroborated by information provided by other CIs, cellular phone records and/or other collected evidence.

34. On or about December 4, 2015, APD Detective J. J. Schmidt learned from Enterprise Rental Car Corporation (Enterprise) that Onyeri's father, Innocent Onyeri (Innocent), rented a vehicle on November 3, 2015, from a Houston area Enterprise location. Detective Schmidt then made contact with the manager of the specific Enterprise location in Houston, Texas. The Enterprise manager advised that Innocent Onyeri rented a silver 2015 Mazda 3 sedan, which was picked up on November 3, 2015, and returned on November 7, 2015. The Enterprise manager advised that the silver 2015 Mazda 3 was returned by "Innocent's son", who was with two other black males. The Enterprise manager specifically remembered this return because the vehicle had marijuana residue scattered inside the vehicle.

35. Affiant has spoken with FBI personnel with specialized training in extracting evidence from mobile devices. Per these discussions, your affiant believes there may be evidence still present and accessible on the four devices that were broken by Onyeri and his associates, as well as the fifth device seized from Onyeri's residence.

36. The Devices are currently in the lawful possession of the FBI. The five Devices were seized by Houston Police Department (HPD) pursuant to two Harris County search warrants: (1) A warrant for the 2012 Dodge Charger with Texas License Plate number DBP8855; and (2) A warrant for the Onyeri residence at 12383 Wellington Park, Houston, Texas 77072. The Devices were transferred to APD, which then transferred the Devices to the Travis County District Attorney's Office (TCDAO) for digital forensic examinations. The TCDAO had limited success in exploiting the Devices. The Devices were then returned to APD which subsequently provided them to your affiant. A federal search warrant is being sought out of an abundance of

caution so that further forensic examinations of the Devices will comply with the Fourth Amendment and other applicable laws.

37. The Devices are currently in storage at the FBI Austin Resident Agency, located at 12515 Research Boulevard, Austin, Texas, within the Western District of Texas. In my training and experience, I know that the Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the FBI.

TECHNICAL TERMS

38. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing

dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets,

and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

h. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP

addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

39. Based on my training and experience, I know that the Devices typically have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device and evidence of association.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

40. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

41. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the Offenses described on the warrant, but also forensic evidence that establishes

how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

c. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

42. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examinations of the Devices consistent with the warrant. The examinations may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

43. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

44. I submit that this affidavit supports probable cause for a search warrant authorizing the examinations of the Devices described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

45. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is

relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

Daniel D. Brust]
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on October 3rd, 2016:

UNITED STATES MAGISTRATE JUDGE

Mark Lane
United States Magistrate Judge

ATTACHMENT A

1. The devices to be searched are as follows: 1) SAMSUNG GALAXY NOTE 5 WITH SIM CARD 8901260415764302408; 2) APPLE IPHONE MODEL A1586 WITH IMEI 352061066787330; 3) APPLE IPHONE MODEL A1524 WITH IMEI 354376061250144; 4) ALCATEL ONE TOUCH 665A WITH IMEI 013088004400263 AND 5) SAMSUNG GALAXY NOTE 4 WITH SIM CARD 8901260312783924447. The Devices are currently stored at the FBI's Austin Resident Agency, located at 12515 Research Boulevard, Austin, Texas.

2. This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of Conspiracy to Conduct or Participate in an Enterprise Engaged in a Pattern of Racketeering Activity, in violation of Title 18, United States Code 1962(d), Conspiracy to Commit Wire Fraud, in violation of Title 18, United States Code 1349 and 1343, Aggravated Identity Theft, in violation of Title 18, United States Code 1028A(a)(1), and Attempted Capital Murder, in violation of Texas Penal Code and involve Chimene Onyeri, Marcellus Antoine Burgin and Rasul Kareem Scott and any known or unknown accomplices, co-conspirators, witnesses, victims and/or criminal associates, including evidence, fruits and instrumentalities of the offenses described herein, including but not limited to contact lists, call logs, voicemails, e-mails, files, communications, records, text messages, photos, audios, videos, images, notes, Internet browsing data, device data, operating system data, application data network data and locational data related to and in furtherance of the offenses described herein, in any form.

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

SEALED

IN THE MATTER OF THE SEARCH OF §
§
1. Samsung Galaxy Note 5 with Sim Card § NO. A:16-m-733
8901260415764302408; §
2. Apple Iphone Model A1586 with IMEI §
352061066787330; §
3. Apple Iphone Model A1524 with IMEI §
354376061250144; §
4. Alcatel One Touch 665A with IMEI §
013088004400263; and, §
5. Samsung Galaxy Note 4 with Sim Card §
8901260312783924447, §
all currently located at the Federal §
Bureau of Investigation, Austin, Texas. §
§

MOTION TO SEAL THE APPLICATIONS AND AFFIDAVITS FOR SEARCH WARRANTS AND THE SEARCH WARRANTS

Comes now the United States of America, by and through the United States Attorney for the Western District of Texas, and respectfully requests the Court to order this Motion, the Applications and Affidavits for Search Warrants, and the Search Warrants filed in the above-styled and numbered cause be SEALED for thirty (30) days from the date of this Order, save for two copies of each to be issued to the Affiant and one file-stamped copy of each to be provided to the United States Attorney's Office.

As reason for such request, the United States would show that the criminal investigation remains pending and may be jeopardized if the information contained in the foregoing document is not sealed.

RICHARD L. DURBIN, JR.
United States Attorney

By: 

Gregg N. Sofer
Assistant United States Attorney

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

SEALED

IN THE MATTER OF THE SEARCH OF	§	
	§	
1. Samsung Galaxy Note 5 with Sim Card 8901260415764302408;	§	
2. Apple Iphone Model A1586 with IMEI 352061066787330;	§	NO. A:16-M-733
3. Apple Iphone Model A1524 with IMEI 354376061250144;	§	
4. Alcatel One Touch 665A with IMEI 013088004400263; and,	§	
5. Samsung Galaxy Note 4 with Sim Card 8901260312783924447,	§	
all currently located at the Federal Bureau of Investigation, Austin, Texas.	§	
	§	

ORDER

Before the Court is the Government's Motion to Seal the Applications and Affidavits for Search Warrants and the Search Warrants in the above-styled case, and after considering the same, the Court is of the opinion that it should be granted in the interest of law enforcement. Accordingly,

IT IS ORDERED that the Clerk of the Court file the Applications and Affidavits and the Warrants UNDER SEAL for a period of 30 days. Should the government wish the warrant documents to remain sealed thereafter, it must file a motion seeking that relief in a manner consistent with the Standing Order of this Division on the sealing of warrants. Failure to seek the continuation of sealing will result in the warrant documents being unsealed.

IT IS FURTHER ORDERED that the Government's Motion to Seal, as well as this order shall remain sealed until such time as the remaining warrant documents are unsealed.

SIGNED this 3RD day of October, 2016.

UNITED STATES MAGISTRATE JUDGE

Mark Lane
United States Magistrate Judge

D1SW15100715

No:_____

THE STATE OF TEXAS	§	IN THE 403rd JUDICIAL
V.	§	DISTRICT COURT
_____	§	TRAVIS COUNTY, TEXAS

ORDER ON STATE'S MOTION TO SEAL

On this the 10th day of November, 2015, came on to be heard the State's Motion to Seal and the Court finds good cause exisis and therefore orders that the above referenced Probable Cause Affidavit and Search Warrant to be sealed for 30 days.

Judge Presiding
403 District Court
Travis County, Texas

Filed in The District Court
of Travis County, Texas
NOV 10 2015
At 2:58 P M.
Velva L. Price, District Clerk

D1SW15100715

IN RE	§	IN THE DISTRICT COURT
SEARCH WARRANT	§	_____JUDICIAL DISTRICT
	§	TRAVIS COUNTY, TEXAS

STATE'S MOTION TO SEAL SEARCH WARRANT

COMES NOW THE STATE OF TEXAS, by the undersigned Assistant District Attorney and moves the Court to seal the affidavit supporting issuance of a search warrant **S-**_____ issued by the Court on the 10th day of November 2015.

In addition to probable cause supporting issuance of the search warrant described above, the affidavit establishes the existence of a compelling State interest in the confidentiality of information, specifically, that public disclosure of the affidavit would cause the destruction of evidence and possibly lead to the tampering of evidence and/or witnesses.

THEREFORE, the State requests that the affidavit for a search warrant for the above-described premises be sealed for a period of 30 days.

RESPECTFULLY SUBMITTED this 10th dat of November, 2015.

Dayna L. Blazey
Assistant District Attorney
Travis County, Texas

Filed in The District Court
of Travis County, Texas

NOV 10 2015

At 2:55 P M.
Velva L. Price, District Clerk

D1SW15100715

SEARCH WARRANT NO:_____

COUNTY OF TRAVIS	§	IN THE DISTRICT COURT
	§	
STATE OF TEXAS	§	403rd JUDICIAL DISTRICT

WARRANT for Electronic Customer Data

The State of Texas: To the Sheriff or any Peace Officer of TRAVIS County, Texas, or any Peace Officer of the State of Texas:

Whereas, the affiant whose name appears on the affidavit attached hereto is a peace officer under the laws of Texas and did heretofore this day subscribe and swear to said affidavit before me, and whereas I find that the verified facts stated by affiant in said affidavit show that affiant has probable cause for the belief he/she expresses herein and establishes existence of proper grounds for issuance of this Warrant for Stored Customer Data or Communications under Article 18.21, Section 5A of the Texas Code of Criminal Procedure and the reciprocating statute of:

- ☐ New Jersey under N.J.S.A. 2A:156A-29(e)
- ☐ California under PC 1524.2
- ☐ Massachusetts under MGL 276, Section 1B
- ☐ Hawaii under Act 325
- ☐ Virginia under Criminal Procedure Section 19.2
- ☐ Florida under 92.605
- ☐ Minnesota under 626.18
- ☐ Washington Criminal Procedure Section 10.96
- ☒ New Jersey under N.J.S.A. 2A:156A-29(e)

Now, therefore, you are commanded execute this warrant by serving it upon the below-listed provider through any permissible means pursuant to the Texas Code of Criminal Procedure Article 18.21, Section 5A,:

T Mobile
4 Sylvan Way
Parsippany, New Jersey, 07054

The employees or agents of the above-listed provider are hereby ordered to furnish the Affiant hereof with the following electronic customer data from the providers' electronic storage as required by the Texas Code of Criminal Procedure Article 18.21 and 18 U.S.C. § 2703,:

Filed in The District Court
of Travis County, Texas
NOV 10 2015
At 2:58 P M.

Electronic Customer Data relating to phone number(s) (832) 335-2534 held in electronic storage by T MOBILE or its subsidiaries, agents, or assigns,

And to seize, secure, analyze, tabulate and make return thereof according to law, the following property or things, for the time period of **October 1, 2015 through November 10, 2015** and with regard to the above listed cellular phone number(s):

direct connects/walkie-talkie details/chirp numbers, call details, caller identifications, payment information, any and all account information and/or account notes, and, cellular site records, including any and all ranging [real-time-tool (RTT)] "RTT data", "reveal" (per-call measurement data) in unabridged format call detail location records with cell site and sector (including interim, hand-off cell sites and sectors from the durations of calls), "angle from the tower" data information which may be available for up to twelve months prior to the date and time of issuance of this Order, (or the beginning of the accounts/whichever is latest) pertaining to the cellular telephones/landline telephones, voice over internet protocol (VoIP) device numbers listed on the front page of this order, or, any telephone/pager/communications device, account, email address, Internet Protocol (IP) address, etc., numbers/identifiers revealed from the original target number records.

Subsequent sections provide more technical details as to what precisely is ordered to be released for the time period authorized by this Warrant that is noted previously.

The following involves technical language in recognition of the cellular and related technologies in use today which may have been involved in the providing of services to the target devices. The Warrant requests the release of subscriber information, unique account and equipment identifiers (phone and equipment serial numbers), *and*, network addressing and routing information. Also requested is the release of cell site, or antenna, information for communications activity. This information typically identifies the cellular antenna used to process a communication event. This Warrant does not require the release of the contents of any communications or order the release of any real-time information or the release of any information documented after the date and time of the issuance of the Warrant.

The following is required to be provided, if available, for the dates and times specified in this Warrant:

1.) Cell sites activations, including any available ranging data [distance from tower, range to tower (RTT)], and all registration information, including signal strengths, logs, etc. (if obtainable), including any location information delivered to a public safety answering point (PSAP) pursuant to a 911 call.

2.) All outgoing and incoming communications/call detail records (CDRs), with cell sites, including all telephone numbers, chirp numbers/direct connects/walkie-talkie/Universal Fleet Mobile Identifier (UFMI) numbers, email addresses (electronic mail), Internet Protocol (IP) addresses, World Wide Web (www) addresses, dialed/communicated with (outgoing and/or incoming). This includes local and long distance telephone connection records, including all text [short message service SMS)] detail records, email detail records [including IP (Internet Protocol)] logs, email header information, and email addresses], IP connection detail records/logs, *and*, video, audio, and/or photo image transactions records, such as multimedia messaging service (MMS) (picture/video messaging) detail records/logs, sent or received, to provide dates, times, and methods of voicemail access, including all available SS7 signaling records of these communications, and, records of session times and durations.

3.) All subscriber information, including any available telephone numbers, email addresses, IP addresses (including ports), etc., and/or unique account, equipment, and/or network addressing, these may include the Electronic Serial Number (ESNs), International Mobile Subscriber Identifier (IMSIs), Temporary Mobile Subscriber Identity number (TMSI), International Mobile Equipment Identifiers (IMEIs), Mobile Equipment Identifiers (MEIDs), Mobile Station Identifiers (MSIDs), Mobile Identification Numbers (MINs), Mobile Dialed Numbers (MDN), Integrated Circuit Card IDs (ICCIDs), Personal Unlocking/Unblocking Codes (PUKs), PINs (personal identification numbers), Blackberry PINs (personal identification numbers/codes), Apple's Unique Device Identifier (ID) (UDID), and/or Media Access Control (MAC) address(es), and all billing/payment information and accounts notes, for the specified cellular/wireless telephones, and, for any other cellular/wireless telephones on the same account as the target numbers, or, any identified telephone numbers, IP addresses, UFMI numbers, email addresses, etc., revealed from the original target phone's records.

4.) If available, an engineering map; showing all cell-site antenna/tower locations, sectors, azimuths, beam widths, pilot PN (pseudo noise) offsets, and true orientations. And, a list of any and all cellular sites numbers [Local Area Codes (LACs), Cellular Identifiers (CIDs), IAP (intercept access points) system identities, repolls, switches, etc], locations, addresses, neighbor lists, etc., and/or latitude and longitude of any said sites. Also, that cellular sites lists, including latitudes and longitudes, be provided, via electronic mail, or via shipping when email is not available, in an electronic format, if available and/or possible. Furthermore, the concerned carrier(s) will provide RF (radio frequency) propagation maps/surveys and cellular antenna/tower maintenance records, and, cellular antenna/tower maintenance records procedures, upon request. These

maps/surveys and maintenance records will be provided in electronic format, such as original color format, if available.

5.) Should the cellular/wireless number/equipment which is the current target of this Warrant have changed, during the requested period, including the MINs/MSIDs, MDNs, ESNs, MEIDs, IMEIs, IMSIs, ICCIDs, PUKs, IP addresses, UDIDs, PINs and/or MAC addresses, or combinations thereof, have been changed by the subscribers during the period of time(s) covered by this Warrant, then this Warrant will apply to any other MINs/MSIDs, MDNs, ESNs, MEIDs, IMEIs, IMSIs, ICCIDs, PUKs, IP addresses, UDIDs, PINs, email addresses, and/or MAC addresses.

6.) That, any Internet Service Provider (ISP), email company or email server entity (public or private), website hosting company, and/or website or internet service providing company and/or entity, provide any subscriber information, email addresses, email logs (with header information, but without any content such as subject lines or the body of emails), Internet Protocol (IP) logs, website addresses, etc., for any email addresses, IP addresses, user names, etc., identified from the original records pertaining to the target devices. Such as, if the original target devices' records reveal Internet activity, such as email activity, web activity, and/or other Internet connected applications, then this Warrant will also order the release of all subscriber information pertaining to user identifying, *and*, addressing and routing (transactional) information pertaining to that Internet activity (without content information) for the effective period of this order. This includes application of this Warrant to Microsoft's "Sidekick"/"Danger" products/services.

7.) Also, that, whenever possible, that the provider(s) provision, upon the specific requests of the prosecutors/officers/agents/designees, a twenty-four (24) hour switch-technician/employee/vendor to assist in providing data to comply with this Warrant and/or the interpretation of the provided data.

8.) That, with applicable formats, that the providers supply upon the specific request of the officers/agents/designees, IMSIs and IMEIs, when applicable, and also will provide TMSI information as often and/or frequent as it should have changed, if applicable and upon the specific requests of the investigating officer.

9.) That, any so ordered providers, or those possessing said information, provide any required information on demand, if possible and upon the specific request of the investigating officer. Further, that any so ordered provider(s), or those possessing said information, provide, upon the specific request of the prosecutors/officers/agents/designees, any historical geo-location services/global positioning system (GPS) data/enhanced 911 (E911) records which may be available to any involved provider(s) and/or parties.

10.) That all call/communication detail, direct connect, subscriber, numeric messages, alpha-numeric/text messages, email records, IP logs, etc., and any related records and/or access be provided, upon the specific request of prosecutors/officers/agents/designees of specific data from specific time period within the confines of this Warrant, in an electronic format specified by prosecutors/agents/officers/designees. Also, that the records/data, be forwarded via email (in a common electronic format as described in section 11) if possible, upon the specific request of the investigating officer, to the listed officer and/or his/her designees. These designees may include, but are not limited to, officers/agents/designees and/or representatives of the Austin Police Department, Travis County, Texas Sheriff's Office, Texas Department of Public Safety, United States Attorney's Office, Federal Bureau of Investigation, United States Secret Service, United States Marshals Service, United States Immigration and Customs Enforcement, United States Department of Homeland Security, United States Drug Enforcement Agency, United States Postal Inspections Service, etc.

11.) If e-mail is not available/possible, that the providers provide the required data electronically on a common storage medium, such as CD-ROM (compact disc read only memory) discs, and/or floppy discs. Also, that all providers provide, when possible and so requested, all requested data in ASCII, comma separated values (.csv), or fixed length (SDF) format. This is to include that any and all records/data will be provided in all available formats of data, upon request, to include, but not limited to, documents/files currently produced in Microsoft Word, Microsoft Excel, PDF (portable document format), CSV (comma separated value), other electronic formats, and/or pulled from such systems such as "CDR Live", "X-Mine", "CEER", and any other electronic medium that is/was in use and/or in development. All CDRs [call/communication detail records (CDRs), including IP (internet protocol) logs, email logs, etc.] will be provided in spreadsheet (Excel, CSV, etc.) format if possible. Only where this is not possible, to provide information in dark, clean typeface, machine-scanable/Optical Character Recognition (OCR) interpretable hardcopy. This includes the faxing of any necessary requested records at the highest possible quality setting. Further, that upon the specific request of prosecutors/agents/officers/designees, that any provided data, including account specific data and cellular site lists, be provided by the necessary providers in a business records affidavit format that complies with the laws of the State of Texas.

12.) Communications providers, companies, and entities are also ordered to provide any and all data and services that are ordered herein, verbally, to prosecutors/officers (or designees) if specifically requested to do so. Communications providers are also ordered to notify prosecutors/officers (or designees) if devices roamed (and what specific networks are roamed to/from) from a home/primary network to another network and it is known by the home/primary network to what roaming network the devices roamed. This includes verbally notifying prosecutors/officers (or designees) of the last known network registrations/activity for the time period specified in this Warrant. And,

if the accounts were active accounts, including if the account was inactivated or closed for non-payment, and, how many minutes and/or credits remained on prepaid type accounts. The concerned communications carriers are also ordered to retain, indefinitely, hard and soft copies of all records and/or data provided as a result of this Warrant.

13.) That any applicable communications provider is ordered to provide all addressing and routing information associated with installed applications on the target devices that are the subject of this Warrant, including but not limited to all Apple "i" products, Google Android "Market Apps", *or*, any other applications not listed herein but that are installed on said device(s).

14.) It is also ordered that all involved communications providers and associated retailers/companies are ordered to release, upon specific request, all purchase, payment (cash, credit, check, prepaid card, etc.), and activation information (even if through third parties) for all target devices, accounts, and subsequent payments, such as prepaid minute cards. This includes the specific data, time, location (including the specific store, register, clerk, etc.) that all devices, account changes, purchases, payments, etc., occurred. It is also ordered that all involved retailers (and neighboring businesses/residences) release any available surveillance video from the aforementioned transactions, both from within, and from the outside of the stores, and the area of the stores, where any of the aforementioned transactions occurred.

Finally, this Warrant will apply to any and all companies/entities which may provide and/or carry wireless/telecommunication services for the target mobile numbers/unique account identifiers/equipment, and/or, any other entity who may possess the requested information, such as Internet companies/entities. This may be required because of number portability and/or if the original carrier was modified due to roaming and/or other considerations/reasons.

Once said electronic customer data has been furnished to Affiant, herein fail not that you shall make due return thereon to this magistrate showing how you have executed same.

Issued this the 10 day of November 2015, at 7:46 AM/PM

District Court Judge
Travis County, Texas

D1SW15100715

SEARCH WARRANT NO:___ _____

COUNTY OF TRAVIS	§	IN THE DISTRICT COURT
	§	
STATE OF TEXAS	§	403rd JUDICIAL DISTRICT

AFFIDAVIT FOR SEARCH WARRANT
FOR TELECOMMUNICATION RECORDS

Joanna Candoli, a detective with the **Austin Police Department** and authorized peace officer under the laws of the State of Texas, now appears under oath before the undersigned Judge and requests the issuance of a Search Warrant, to search the following:

Electronic Customer Data relating to phone number: (832) 335-2534 held in electronic storage by:

T Mobile
4 Sylvan Way
Parsippany, New Jersey, 07054

And to there seize, secure, analyze, tabulate and make return thereof according to law, the following property or things:

to include call detail records, for the time period of October 1, 2015 through November 10, 2015 and with regard to the above listed cellular phone number(s):

direct connects/walkie-talkie details/chirp numbers, call details, caller identifications, payment information, any and all account information and/or account notes, and, cellular site records, including any and all ranging [real-time-tool (RTT)] "RTT data", "reveal" (per-call measurement data) in unabridged format call detail location records with cell site and sector (including interim, hand-off cell sites and sectors from the durations of calls), "angle from the tower" data information which may be available for the time period specified in this warrant pertaining to the cellular telephones/landline telephones, voice over internet protocol (VoIP) device numbers listed in this warrant, or, any telephone/pager/communications device, account, email address, Internet Protocol (IP) address, etc., numbers/identifiers revealed from the original target number records

Filed in The District Court
of Travis County, Texas

NOV 10 2015

At 7:58 o'clock

The following facts having been sworn to by Complainant in support of the issuance of this Warrant:

Your affiant is the detective for the Austin Police Department Tactical Intelligence Unit and member of the US Marshals Lone Star Fugitive Task Force. Our unit was asked to assist the Austin Police Homicide Unit on an Attempted Capital Murder offense.

On 11/06/2015 Austin Police Officers responded to a report of a shooting at [redacted], Austin, Travis County, Texas. A female victim had been shot in the driveway of her residence by a male dressed in all black. The victim, Travis County District Court Judge J. Kocurek, had just returned home from a sporting event with her family members. They did not recognize the suspect and did not know of any motive for the shooting, aside from the victim's profession. This offense is being investigated under APD case # 2015-3101943.

The victim was transported to the hospital with serious injuries and Austin Police Homicide detectives responded to assist with the investigation. A canvass of the area and interviews with neighbors yielded information that an unknown black male had been sighted in the immediate area prior to and on day of the shooting. APD 911 and 311 calls showed neighbors had made suspicious person reports of a silver sedan driving in the immediate area two days prior to the shooting and a black male wearing a mask running through yards the morning of the shooting.

Homicide investigators began researching any threats made against judges in the area. One particular threat was recent: on 10/16/2015, an unidentified [redacted] called the Travis County District Attorney's office and gave information about a male who was threatening to kill a judge. The male was identified as ONYERI, CHIMENE, black male, date of birth [redacted]. The caller reported [redacted] had heard ONYERI make the threat. ONYERI, who lives in Houston, Texas, had previously been arrested for fraud in Rollingwood, Travis County, Texas in 2012. ONYERI was placed on deferred adjudication for that offense. ONYERI was subsequently arrested for fraud charges in Louisiana and violated the conditions of his deferred adjudication on the Rollingwood case. On 08/29/2015 a warrant was issued for ONYERI out of Judge Kocurek's court. ONYERI's case was set on Judge Kocurek's docket for 10/7/2015 at the Travis County courthouse and the case was reset. It is unknown if ONYERI had any contact with Judge Kocurek at this time. That was the extent of the victim's dealing with ONYERI.

The [redacted] tipster called back after the shooting and ended up leaving a message on a courtroom bailiff's phone. It was not listened to until Monday 11/09/2015. [redacted] reiterated that ONYERI had threatened to shoot a judge and that ONYERI confessed to a third person that he shot the judge here in Austin.

On 11/08/2015, the USMS in Houston, along with the Houston Police Department, conducted surveillance on five addresses associated with ONYERI. ONYERI, who had an outstanding felony Larceny warrant out of Louisiana, was arrested after he was spotted in a vehicle leaving one of the addresses.

Houston Task Force officers interviewed Innocent Onyeri, the father of ONYERI. Innocent provided officers a phone number for ONYERI from the address book of his cell phone. That number, (832)-335-2534, is serviced by T Mobile. Just prior to ONYERI being taken into custody, Task Force officers observed him breaking a cell phone he had in his possession. Your affiant believes that ONYERI was aware incriminating evidence will be recovered in his phone and was attempting to destroy it.

Your affiant is requesting subscriber information and historical call detail records with locations for this number for the time frame of October 01, 2015 through November 10, 2015 in order to show the locations of ONYERI's phone. Your affiant believes the records will show whether the phone used by ONYERI traveled from Houston to Austin in October for his court case and in November around the time of the shooting.

WHEREFORE, your Affiant requests that a Judge issue a Search Warrant directing a search for and seizure of the items/property described above.

Affiant

Subscribed and sworn to before me on this 10 day of November, 2015.

Presiding Judge

167th Judicial District Court Travis County Texas